MULTIMEDIA UNIVERSITY

STUDENT ID NO

MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 1, 2018/2019

TDF3241 – DIGITAL FORENSICS

(All Sections / Groups)

16 OCTOBER 2018
9.00 AM – 11.00 AM
(2 Hours)

INSTRUCTIONS TO STUDENTS

1. This Question paper consists of 4 pages (including cover page) with 5 Questions only.

2. Attempt **ALL** questions. The distribution of the marks for each question is given. This paper carries **50 marks**.

3. Please print all your answers in the Answer Booklet provided.

Question 1 (10 Marks)

(a) Ali was instructed to conduct a private investigation on industrial espionage. Explain the main characteristics of a private investigation. [4 marks]

(b) You have been asked to present the findings of your investigation in court. Present FOUR (4) steps you should take when preparing for a testimony as a technical witness. [4 marks]

(c) You are required to prepare a forensic report on a case. Demonstrate how to use supportive material on a report. [2 marks]

[TOTAL = 4 + 4 + 2 = 10]

Question 2 (10 Marks)

(a) The prosecution lawyer is preparing a deposition of the key witnesses. Differentiate between discovery deposition and testimony preservation deposition. [4 marks]

(b) You are required to prepare a forensic report to present your findings on a case.Work out what you need to consider in the quality of your writing in order to produce clear, concise reports. [4 marks]

(c) A high profile criminal case usually attracts a lot of attention especially from the media. Propose TWO (2) reasons to avoid contact with news media during a case. [2 marks]

[TOTAL = 4 + 4 + 2 = 10]

Continued ...

Question 3 (10 Marks)

(a) These are many tools available to help you do a forensic analysis. You have been asked to propose some tools to be purchased for your new forensics lab. Classify the FIVE (5) major functions of any computer forensics tool.

[5 marks]

(b) You are a criminal trying to hide your child pornographic materials in your computer. Demonstrate how you can hide data by marking bad clusters.

[4 marks]

(c) Show how vector quantization (VQ) compresses data. [1 mark]

[TOTAL = 5 + 4 + 1 = 10]

Question 4 (10 Marks)

(a) You are a lab manager in charge of a medium sized computer forensics lab. Demonstrate a proper way of disposing materials on your computer investigation lab. [3 marks]

(b) Your company is drafting a security policy to protect company interests and company data. Justify why companies should publish a policy or a warning banner stating their right to inspect computing assets at will. [4 marks]

(c) Journaling is an important feature of a computer forensics investigation. Demonstrate how to use a journal when processing a major incident or crime scene. [3 marks]

[TOTAL = 3 + 4 + 3 = 10]

Continued ...

Question 5 (10 Marks)

(a) You are at the crime-scene. You have been assigned to process the crime scene and to collect evidence. Apply FOUR (4) considerations you should have when deciding what data-acquisition method to use on your investigation. [4 marks]

(b) A hacking intrusion attempt is currently happening on your company network and you have been called to collect evidence to catch the criminal. Prepare the standard procedure for network forensics investigations. [5 marks]

(c) Explain logical cluster numbers (LCNs). [1 mark]

[TOTAL = 4 + 5 + 1 = 10]

END OF PAPER